

U.S. Department of
Justice

Federal Bureau of
Investigation

FBI Bomb Data Center

Physical Security Guidelines

Contents

Security
Planning

Access Denial

Identification &
Interior
Movement
Control

Structural
Enhancement of
Security

Appendix

A bomb threat is an excellent means of disrupting business and lessening efficiency in any agency. The problems are intensified when the incident involves an actual explosive or incendiary device. Private institutions, commercial concerns, and government agencies often request aid from public safety and law enforcement organizations in evaluating existing security programs and developing new preventive measures against bomb attacks on their premises. To meet this continuing need, the Bomb Data Center (BDC) has completed a series of publications addressing security against bomb attacks. The seven bulletins have been combined in this pamphlet.

The purpose of the pamphlet is to provide BDC participants with background information and an outline of the basic planning and preparations necessary to assist the public in making effective arrangements; and to aid law enforcement agencies in effecting the protection of their own facilities against explosive and incendiary attacks. Material in the pamphlet concerns security planning, assessments, policies, and some methods of implementing adequate security. Procedures to be implemented following the discovery of a bomb are not addressed. The recommendations, both general and specific, made herein are intended as guidelines to intelligent action based on a comprehensive review of a specific situation. Every point is not universally applicable. In addition, priorities and techniques should be assessed with respect to the perceived risk, as well as the availability of funds, manpower, and time.

Security Planning Phase

In general, security planning measures for the prevention of bombing and other attacks should be based on several concepts which eventuate in the planning steps outlined below. Security planning should be regarded as a cyclical procedure. [Figure 1](#) illustrates six sequential steps that must be repeated periodically in order to assure an adequate degree of security preparation. These steps are:

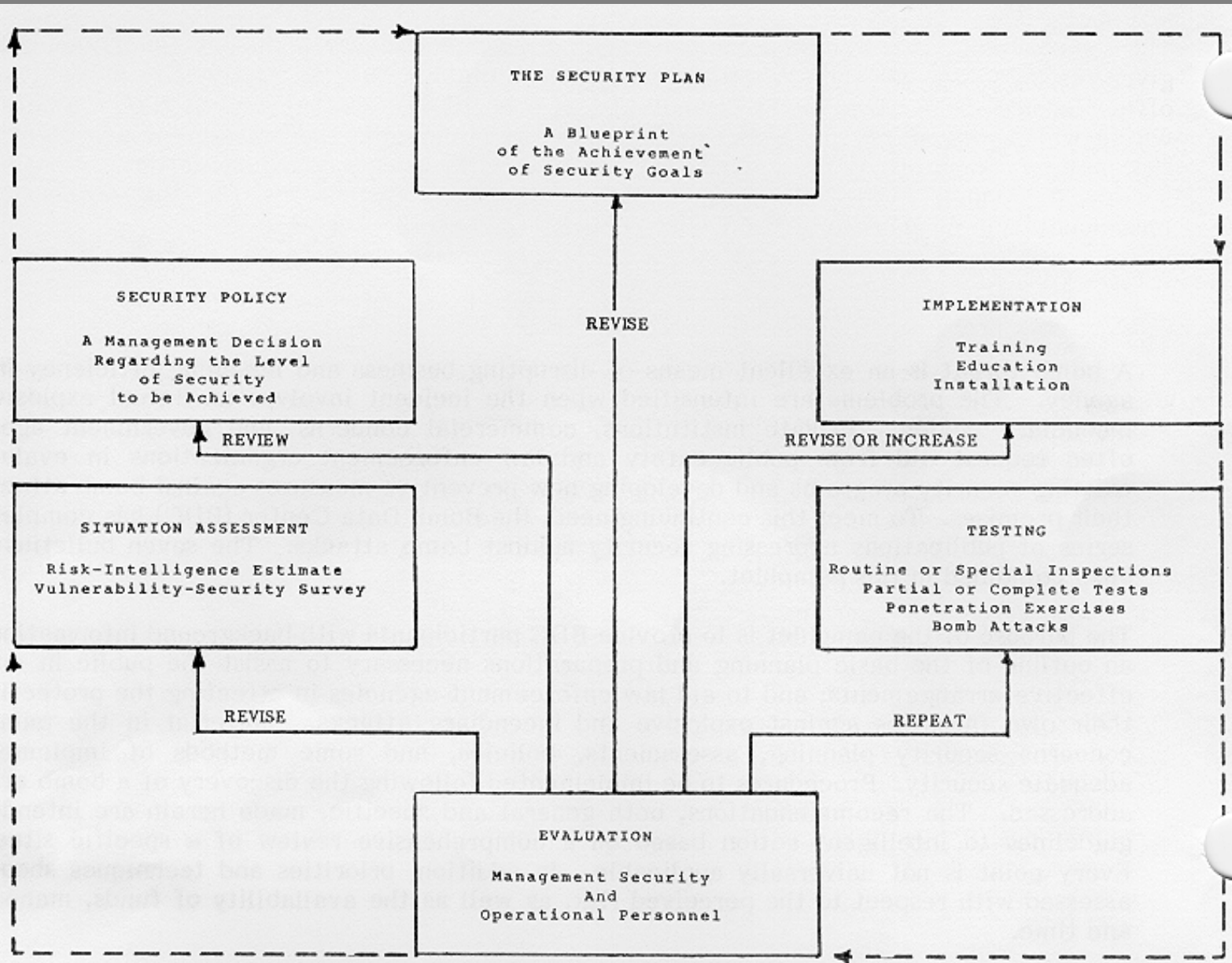
1. [Assessment of the Situation](#)
2. [Security Policy Formulation](#)
3. [Security Plan Development](#)
4. [Plan Implementation](#)
5. [Inspection and Testing](#)
6. [Evaluation](#)

The Security Officer

Adequate leadership is essential to the success of any security plan. Whether security planning and techniques are a full-time assignment or supplementary duties of the selected officer, this individual should be chosen on the basis of background, experience, and interest. (The latter point is an important attribute. An interested and committed officer will be able to inspire a great degree of confidence and voluntary compliance among other personnel.) In large or decentralized agencies, it may be necessary to appoint security officials for each area/location, since they must be familiar with the facilities and personnel within their respective areas of responsibility. In most cases, the command organization for security personnel will follow existing patterns. In a police or fire department, for example, a security officer might be appointed for the headquarters facility, with assistants named for precincts or stations. For decentralized agencies which have been determined to be high-risk premises, such as police departments in high-crime areas, a full-time security officer may be feasible. Under these circumstances, selected personnel in other facilities, less susceptible to attack, may only be assigned security as an additional responsibility.

[Contents](#)

The security officer, subject to the supervision of agency management personnel, should be given responsibility for the overall development and administration of security plans. This officer should be involved in the formulation of security policies, as well as the parameters within which procedures are to be implemented. For example the assessment of potential risk may be conducted by the security officer, who will report the findings to the responsible agency personnel. The officer should also be made responsible for the design and implementation of plans to be used when security has been breached.

Figure 1. Steps in Security Preparation**FIGURE 1.**

Assessment of the Situation

The entire security program for any agency derives from a determination of the inherent risk and vulnerability. These assessments will be affected by the general scope of security measures already in practice at the premises, and by the sensitivity of the operations conducted therein. The evaluation will serve three general purposes.

1. It will assure that security plans are appropriate to the area being protected.
2. It will serve as a basis on which to formulate a security policy and plan that is proportional to the existing or potential threat.
3. It will provide for updating or revising plans to include appropriate countermeasures for new hazards.

The evaluation will be a continuing process, and will include such data as relevant criminal trends, the sensitivity of the business conducted, and the types of security measures already being implemented.

Relevant Trends - This facet of the operation involves determining the history of bombings and sabotage against the kind of organization under evaluation, as well as against the specific agency. Background information on criminal trends can sometimes be obtained from local law enforcement units, the news media, or neighborhood associations. The BDC can occasionally provide specific information which will indicate trends among its contributing membership. Information relative to thefts and recoveries of explosive materials is currently collected by the Bureau of Alcohol, Tobacco and Firearms (ATF), U.S. Department of the Treasury. Project SEAR (Stolen Explosives and Recoveries), which was begun by ATF in 1976, gathers and computerizes information regarding stolen and recovered explosives. This enables ATF to readily assist local, state, Federal, and foreign agencies in the investigation of explosives-related incidents. One of the purposes of Project SEAR is the establishment of trends and patterns for explosive thefts.

Background information of other types may also be useful. For example, the presence of organizations that foment unrest in the community should be noted, particularly if the nature of the organization's business is likely to inspire animus among segments of the population. An assessment should also

be made of the technology and materials available in the community to would-be bombers. In areas that support a major mining or construction industry, for example, blasting materials may be readily obtainable.

If the specific agency has been the target of bombers or saboteurs in the past, these incidents should be studied to determine if any areas of poor security or particularly appealing targets are indicated.

Security Survey - When the collected data indicates a substantial hazard for the agency, a comprehensive physical security survey should be conducted, to identify security hazards or deficiencies, and to develop recommendations for minimizing or eliminating the opportunities for an attack.

In order to assure that the recommendations made are appropriate, practical, and cost effective, the survey should be conducted by personnel who are experienced in security matters; it may be assigned to the security officer, if one has been designated. As an alternative, the physical security survey may be conducted by a professional security consultant or on a contract basis. Under these circumstances, a project manager or other agency official should be designated to administer the task.

The responsible personnel should complete the following six preliminaries prior to the start of the survey.

1. Have a meeting with agency management officials to arrange for necessary assistance and coordination during the survey.
2. Obtain a working knowledge of the typical functioning of the facility.
3. Whenever possible, obtain floor and ground plans of the site.
4. Review details of previous bombing incidents and significant security breaches at the facility.
5. Review details of relevant incidents at similar agencies.
6. Consider bombing attacks which have occurred in the vicinity.

Survey Parameters - The physical security survey should address three basic areas: the susceptibility of the target to attack, preventive and reactive measures, and cost. A thorough, systematic procedure should be followed. Inspections should be conducted during periods of peak activity, and also

when the area is not in operation. Work and production patterns will help define security needs and goals.

During the survey, the individual processes of the facility should be analyzed to determine the key functional elements which are vital to its inclusive operation. These "common denominators" may not be readily apparent. For example, a chain of operation could begin with individual machines, controlled by electrically powered computers. Sabotage of the machines or computers, therefore, would not be as harmful as an attack against the generator or electrical matrix. One purpose of the survey is to identify these basic areas which require high priority protective measures. An identification procedure is appended to this text. It should also define additional vulnerable points such as circuit boxes, fuel storage areas, vehicle parking lots, and certain offices. The identification and classification of targets will provide a basis for other physical security decisions.

The nature of these targets will, to a large extent, dictate feasible kinds of protective measures. In addition, the surveyors should consider measures that could be implemented following an attack, to mitigate damages and upheaval as much as possible.

As the level of security is heightened, costs increase. The surveyors, therefore, should be prepared to recommend physical security measures which will provide effective and economical protection commensurate with the perceived threat. In some instances, the cost of protecting every part of an agency may be prohibitive. It is essential that the survey indicate the areas of critical importance and relative vulnerability.

A final result of the survey should be a written report containing the following information:

- Date
- Name of surveyor(s)
- Complete address and description of premises surveyed
- Pertinent history
- Identification of critical areas and/or elements
- Current security measures, and evaluations of their effectiveness

- Recommendations

This report will be used by reviewing officials to determine the scope and adequacy of the survey, and to make decisions concerning the security system. The report should be afforded appropriate security, as it will contain potentially compromising details of the agency's operations.

Security Policy Formulation

Security measures always represent a compromise of values: absolute protection against an attack is not usually achievable; and the cost of security normally increases in direct proportion to the protection provided. Since responsibility for the development and implementation of security measures rests with those officials who manage the facility, these individuals should determine, according to the perceived risk, what levels of relative security are acceptable in various parts of the operation. In addition to specific security needs and goals, the policy should also address collateral matters such as the effect of security practices on employee morale and productivity, and the available resources. There may also be legal parameters that should be incorporated into the policy. Security personnel may wish to contact agency or local legal advisors concerning the limits of authority applicable in the particular circumstance.

The security policy should provide for the needs of the agency, but should not exceed those needs. A multilevel security program is often most feasible. This concept is based on a rating of agency areas and/or functions, pinpointed during the survey, according to their respective importance. Maximum effort is then expended in protecting the most crucial operations, areas, and equipment. There are various methods of establishing priorities. See Appendix. Such methodologies, while often defined in terms of equipment, can be modified to incorporate operations and personnel.

It is essential to employee morale that managers and security personnel clearly demonstrate a suitable regard for human safety during every facet of security planning and implementation.

Security Plan Development

The responsible management personnel should develop and publish a blueprint for achieving adequate security. The proposed measures should make maximum use of the existing operational structure: i.e., demonstrated supervisory and technical skills, and materials and equipment on hand. The use of available resources reduces security costs, as well as emphasizing the fact that effective security must involve all personnel.

A detailed, comprehensive practical security plan should be written and implemented. This plan should address the normal functions of the agency or business; it will be less effective if operative only during emergencies. The optimum plan will allocate human and fiscal resources to ensure an acceptable level of physical security. The plan can be very elaborate: some agencies, for example, incorporate a statement of background and goals into the actual documentation of the plan. The sample plan appended to this pamphlet does not include this, although it may be added at the discretion of the responsible personnel.

Plan Implementation

Implementation of a security plan should be undertaken only after management, security, and planning personnel are satisfied with it. The implementation consists of two facets: preparation of required apparatus and systems; and training and education.

The first phase entails not only the installation of new equipment, but also testing and rehabilitation of existing paraphernalia. This might include replacing locks, fences, etc., and verifying that all security equipment functions as intended. Local fire regulations must be consulted; certain security matters may be affected.

Agencywide education and training are essential to the smooth and efficient operation of its security system. This includes not only the training of security guards (if used) and other directly involved personnel, but also a thorough information program for all occupants of the premises. The program should acquaint personnel with the nature and purpose of the procedures, and elicit cooperation during their day-to-day functioning. Security education programs must be supported by top management; any indication of high-level indifference will result in similar attitudes throughout the personnel structure.

Inspection and Testing

A program of inspection and testing will assure that the security plan continues to operate effectively. Periodically, drills planned to demonstrate security preparedness should be conducted. The procedures should be frequently reviewed, tested, and revised as necessary to retain effectiveness. Since operational readiness is essential to adequate security, continuing inspections should occur.

The inspections, which can often be incorporated into existing practices, should be both scheduled and unannounced. They should include all aspects of the implemented plan. In law enforcement agencies, for example, shift or precinct commanders might conduct security inspections of their areas of responsibility as part of routine duty. Specifically appointed security officers would also conduct detailed surveys of selected areas. In every inspection, the emphasis should be on identifying and correcting security weaknesses, rather than determining the extent of employee compliance with the existing plan.

Security plans, such as the one appended to this narrative, which provide for increased levels of security under specified conditions, should be tested through the controlled implementation of these levels. Such tests, which may involve some or all aspects of the plan, should be unannounced and designed to tax security procedures under the most adverse conditions: on a weekend or other period when the agency does not pursue normal operations.

An effective test for a bomb security system is a penetration exercise, in which an individual attempts to breach the security perimeters and place a suspect item within the premises. This is primarily a test of access control and will place the simulated bomber in no risk. If the item is successfully planted, reporting procedures by security personnel or other employees can be evaluated. See Appendix, Alert Condition 1.

The most reliable test of a bomb security system is its functioning during an actual attack. Any bombing attempt against the agency, whether successful or not, should be studied for evidence of security weaknesses. Incidents at allied establishments can also be used for evaluation purposes.

Evaluation

Management, security, and operational personnel should all be involved in the ongoing evaluation of the plan. Assessments may be made not only on the basis of routine operation and testing, but also on the efficacy of the procedures when an actual attempt to breach security parameters occurs. Interested personnel should participate in systematic reviews of all evolving data, in order to determine additional security needs. Without a continuing, systematic, and effective assessment program, security costs may escalate or protection diminish.

Access Denial

A potential bomber must, in most cases, situate all or part of the explosive device at the target area. Therefore, the denial or control of access to the premises is a cornerstone of the bomb security plan. In some cases, severely limiting or denying access is a straightforward part of the agency operation. The sensitivity of the business conducted may dictate limited access, as well as searches of the belongings and parcels of those admitted to the premises. This is a practical and effective technique, which can be easily implemented if a guard or pass/badge system is part of the existing operation. However, there are occupancies where, even though the perceived risk is great, access cannot feasibly be denied. Under these circumstances, movement within the confines of the agency must be controlled. This section of the pamphlet addresses the various degrees and ramifications of access denial.

[Perimeter Barriers](#)

[Sentry Dogs](#)

[Illumination](#)

[Protecting Utility Areas](#)

[Alarms](#)

[Protecting Public Areas](#)

[Security Guards](#)

[Doors and Windows](#)

[Contents](#)

Perimeter Barriers

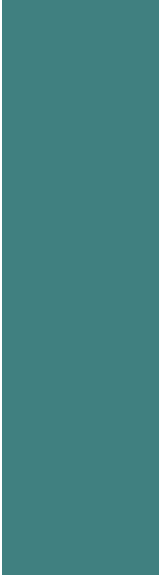
A limit to the area to be considered is indicated by the inclusive enclosure of the agency's operation; it is probably already defined by fences or natural boundaries. In those instances where there are no perimeter barriers, the exterior of the structure serves the same purpose and should be afforded appropriate security. The protection of the existing barriers can often be buttressed by the implementation of some of the measures discussed herein. Natural boundaries, such as bodies of water, are not effective deterrents and should be augmented with guards or artificial barriers.

Fencing: The use of fencing to define and protect a perimeter offers several security advantages. Not only will its use delay unauthorized entry to the premises, the fences will channel traffic and personnel to appropriate access points. Additionally, the number of patrol personnel needed can be kept to a minimum.

Chain link fencing is a commonly used type, and is ideal with respect to permitting unimpeded surveillance of the perimeter area at all times. However, potential bombers and saboteurs are afforded the same opportunity. There are various standards for the installation of fencing. It is most feasible, however, to seek advice from a security professional or knowledgeable individual from an allied agency; available products vary substantially, as do specific security requirements. In general, the fences should be securely installed and adequately braced. The barrier should be kept free of undergrowth. It should be regularly inspected for deterioration or tampering. If fencing crosses a waterway such as a stream, some provisions may be necessary to ensure the structural integrity of the fence, as well as to secure water apertures: i.e., installation of culverts with screened ends.

The incorporation of additional features will augment the fence as an effective barrier to access. An angled arm of barbed wire may be strung along its top edge. A paved perimeter road will provide a clear area and can be used for vehicle patrols. Guards, dogs, mechanical intrusion detectors, or some combination of means may be used at the barrier. One technique is to install parallel fences a few feet apart, with dogs or devices used between. Protective lighting creates a psychological deterrent as well as facilitating visibility.

Masonry walls rather than fencing can be used in some circumstances. The security they afford can be increased by cementing broken glass to the top edges.



Whatever type barrier is used, it should be visible, and the areas adjacent to it free from structures, vegetation, containers, etc. If the area is not paved, it can be surfaced with a light-colored material such as sand, which will improve visibility. Grass in this region should be short, and storage and parking prohibited.

Sewage and drainage pipe, which may violate the security perimeter, should be protected with grids or mesh. Utility tunnels, which provide underground access to service and maintenance personnel, should be similarly secured when accessible from the outside the perimeter.

Illumination

Proper lighting can increase the efficiency of whatever exterior security measures are used. It will serve as a deterrent and will also permit observation of the area by unseen personnel. Professionals should be consulted for help in developing a cost-effective and practical lighting system. As a component of this plan, emergency lighting with an independent power source should be considered.

All apparatus should be inspected regularly to ensure that it is functioning properly. Lamps, for example, should be replaced at whatever percentage of their rated life is recommended by the manufacturer or an electrician; this will minimize dark spots due to burnouts. Fixtures can be secured with the installation of breakage-resistant lenses and wire guards; stanchions can be electrified. A local utility company, which may deal with similar problems, can be contacted for recommendations.


(Protective illumination need not be restricted to exterior, perimeter areas. Stairwells, elevator shafts, restrooms, and other interior public areas can be equipped with very bright indirect lighting.)

Alarms

An intrusion alarm system is designed to detect attempted breaches of boundaries. In order to be effective, it must be suited to the security plan in operation and backed by sufficient trained personnel to deal with ensuing contingencies. There are many types of alarm systems currently available. Interested personnel should consider a broad spectrum of systems to determine which equipment will meet the needs of the agency and be within the prescribed financial boundaries. Advice on alarm systems should be solicited from agencies in comparable circumstances, as well as from manufacturers and security professionals.

Before any investigation of specific systems is initiated, however, a few general decisions must be made. Many of these involve the areas in which the alarm will be operative: i.e., inside, outside, or both. If inside use is planned, the features of the spaces to be alarmed should be evaluated. A motion sensitive apparatus, for example, would not be practical in a room where a forced air system creates substantial currents. The same type of evaluation will be necessary for exterior alarms. Typical weather conditions should also be taken into account. Intrusion detectors can be affected by sound levels, vibrations, radio transmissions and other types of electrical interference. Although a system that is ideal in every other way can sometimes be calibrated to avoid interference, potential difficulties should be considered prior to purchase. This will help assure effective operation of the equipment and will minimize the possibility of false alarms. A preponderance of nuisance' alarms leads inevitably to a casual response by personnel. Furthermore, if the alarms are received by an outside agency, such as a law enforcement or transmitting station, limits or fines for false alarms may be imposed. In addition, the elimination of extraneous causes for false alarms will enable personnel to identify alarms that are being set off deliberately, in order for potential criminals to gauge the system or lull personnel into thinking that every alarm is false. (BDC Editor's Note: Some intrusion detection equipment includes built-in monitoring capabilities for false alarms. The need for this feature can be evaluated prior to purchase.)

Cost will usually be a factor in the consideration of alarm systems. This includes not only the fee for renting or buying the equipment, but also the overall anticipated expenditure. For example, some systems may be easily and relatively inexpensively installed, while others are prohibitively costly to retrofit. The perceived necessity and possibilities for system expansion should also be evaluated. Available warranties and service contracts will affect the financial feasibility of an alarm system.



Following selection and installation of the equipment, it should be tested and serviced regularly by the appropriate personnel. (Some types of apparatus monitor themselves and indicate malfunctioning - like a smoke detector which emits a sound when the battery is losing power.) Plans, wiring diagrams, and specifications for the alarm system should be secured at all times.

Security Guards

A security force that is trained and appropriately equipped can be invaluable in maintaining perimeter integrity. The guards can be recruited from the ranks of agency personnel or hired from a professional firm. If agency personnel are used, concerns which train and deploy guards can provide some guidelines in developing selection criteria and formulating procedures.

Private security forces, particularly if armed, are subject to various laws and regulations. Legal counsel should be taken to define the scope of responsibility for these individuals. If the guards are to be armed, relevant firearms regulations will require careful evaluation.

The orders given to security guards should reflect the policies of the organization and should be concise and consistent. They should be as specific as possible regarding duties, responsibilities, and limits of authority. If the guards are going to patrol the perimeter, there are various ways to enhance their efforts and assure the desired standard of protection. For example, guards may be tasked with checking-in at specified points along their patrol: if anyone is significantly late an investigation is made. Patrols might also report to a central command post at designated intervals. Within whatever limits are established, patrols should be varied or rotated so that they cannot be predicted. Procedures of this kind will maintain both security and the safety of the patrols.

Sentry Dogs

Dogs can be used, either teamed with a handler or alone, to augment the security system. They provide a powerful psychological deterrent to intrusion and may be used to guard the unoccupied premises. If the perimeter boundary consists of parallel fences, the dogs can be permitted to run between them. Whatever the circumstances under which dogs are used, they should be selected to exploit the keen canine senses of smell and sound.

(BDC Editor's Note: The BDC has prepared several documents on the use of dogs as explosives detectors. Some of this information, which is available from the BDC upon request, may be of value in determining the feasibility of canine use as part of a physical program.)

Protecting Utility Areas

The facilities discussed herein are those which may be located outside the physical structure of the organization. Utility functions housed inside these premises, such as communications or computer equipment, are within the purview of internal security.

Transformers: Transformers are often located in underground vaults, in an outside structure, or on concrete platforms. In the first instance, vaults are often equipped with grills facilitating the dissipation of heat and are accessible through manholes. Frequently changed locks should be used to secure these means of entry. Structures housing transformers should be similarly secured. Fencing, security lighting, and patrols can also be used to maintain security. In some instances, the use of sentry dogs or intrusion detection devices may be warranted. Due to the necessity for heat dissipation and accessibility, the use of sandbags or similar items to protect transformers from blast and fragmentation effects is often impracticable.

Connections and Lines: Distribution lines and service connections should be located underground whenever possible, and blueprints which detail their routes should be protected from unauthorized personnel. If use is shared with other agencies, a cooperative security policy must be developed and implemented.

Above-ground pipes and power lines considered susceptible to sabotage can be monitored through air or ground surveillance. The use of guards may be warranted at particularly vulnerable points, or if a threat is received.

If regular or emergency power is generated within the premises, the efficiency of maintained security should be examined and tested periodically, several times each month. It is also a sound procedure to test the systems to be powered by an emergency power source (lighting, alarms, communications, etc.) both individually and inclusively. Structures housing off-premises utility machinery should be patrolled and checked periodically.

Protecting Public Areas

The portions of any structure accessible to the public will be dictated, to a considerable extent, by the type of business transacted. Usually, however, they include lobbies, some corridors, stairwells or elevator cars, and restrooms. Garages, cafeterias, conference areas, and retail stores in a multiple-use structure can sometimes be added to the basic list. Certain other areas, while not precisely public, are also susceptible to attack.

Public lockers provide excellent concealment for bomb devices. If it is not feasible to eliminate them altogether, the threat can be minimized in several ways. The lockers could be relocated in an area where the risk of injury or damage from a detonation is lessened. Alternatively, protection should be added to areas adjacent to their present locale. In any case, master keys should be readily available in order that the lockers can be swiftly opened upon receipt of a threat or under any other suspicious circumstances.

Telephone equipment rooms and maintenance storage areas are often accessible from public corridors. Their doors should be locked at all times; employees using the rooms should include this among their professional responsibilities.

Trash storage and removal areas pose a hazard in many structures, as they are located in public or semipublic areas, often adjacent to unsecured building entrances. Even if access controls are stringent elsewhere, these particular entrances may be neglected due to the massive amounts of material and number of personnel which pass through them. Adequate, efficient monitoring is essential for trash accumulation areas and loading docks.

The trash itself can present security hazards. It may appear at irregular intervals and in unusual places. Nested, empty cartons, packing materials, and other debris abandoned in a room or corridor pending removal provide excellent hiding places for bombs. The presence of trash can also impede an effective search. Trash, and other extraneous materials left in accessible areas should, therefore, be promptly removed.

Lobbies, Public Entry Areas - Much can be done to reduce the number of hiding places in any public area through furniture selection and placement. The use of contemporary furniture, without aprons, cushions, or upholstery can eliminate many places of concealment. Conventional accessories such as ashtrays and trash receptacles can be replaced with glass, clear plastic, or wire mesh counterparts. Furnishings should be grouped away from walls, and

draperies, if any, should stop 12 inches above the floor. Finally, all doors, as well as some wall surfaces, if feasible, should be glass. All such public areas should be brightly lighted, with no dark areas or shadows.

The adequate surveillance of public areas poses several problems. A posted guard, for example, can seldom see the entire area, and may be diverted by activities in one corner or section. The use of closed-circuit television in conjunction with the guard may be feasible. Other security measures that may be practicable include plainclothes guards, two-way mirrors, and inconspicuous vision slots. Posted information concerning the type of surveillance used can be a powerful psychological deterrent. The illusion can be enhanced by the addition of dummy surveillance devices to the area.

If circumstances warrant, clear plastic (polycarbonate, etc.) partitions can be installed to protect employees in public areas. Many banks and post offices use these materials to separate tellers or clerks from customers.

Restrooms: Bombs can easily be concealed in public restrooms: in unlocked, unoccupied stalls; dispensers and trash receptacles; plumbing cabinets; etc. Security personnel should have keys for examining all such enclosures if emplacement of a bomb is suspected. Containers and receptacles can be fitted with plastic liners that can be lifted to determine weight inconsistent with the typical contents. The replacement of waste receptacles and paper towel containers with endless cloth towel dispensers or electric hand dryers can also be effective, although the elimination of all containers in a restroom is practically impossible. Transparent or wire mesh receptacles, as recommended for the lobby areas, can also be used in restrooms.

Suspended, removable ceiling panels are a potential hazard in any area, especially restrooms, which are only sporadically occupied and usually not under security surveillance. The panels should be well secured to deny access to the crawl space above. Plumbing recesses should be similarly inaccessible to the public.

Maintenance personnel, because of the nature of their duties, are familiar with many accessible areas of a structure that may escape routine inspection. These individuals should be asked to note and report unusual circumstances or items. Such requests can be made in conjunction with policy statements concerning the need for locked doors, efficient trash removal, and other security practices.

Parking Areas - A bomb prepared elsewhere can be installed in an

automobile in a matter of seconds; the bomber need not even gain access to the interior. Explosive devices may be situated under fenders, in gas tanks, and on a variety of accessible structural members. Furthermore, an experienced criminal can easily and quickly enter a locked car. Adequate security for individual vehicles is, therefore, difficult to achieve. Access denial is often the most viable means of protecting them.

Secure lots should be provided for employee and visitor parking whenever possible. These facilities should be located a safe distance away from offices and other structures, in order to minimize damage to critical areas in case of a vehicle explosion. Cars should be parked in a manner that will ensure prompt and observable removal during a crisis.

Personnel and vehicle access to parking lots can be controlled by using an identification badge or sticker system. Additional security measures include the installation of fencing, adequate lighting, image sensing equipment, and intrusion detectors. Patrols or guard dogs can also be used.

Boat Areas - Some businesses and law enforcement agencies maintain watercraft and pier facilities which must be secured. Access to these facilities by land can be controlled or monitored by the same means used in other parts of the organization. Different security measures may be needed, however, to protect areas approachable by water. Agencies charged with such a responsibility might contact local yacht clubs, public pier administrators, or U.S. Coast Guard installations for specific, technical devices appropriate for their circumstances.

Doors and Windows

This section addresses the prevention of access through doors and windows that are not intended for entry. Adequately secured doors and windows are especially important when the premises is not surrounded by a perimeter barrier.

Doors - Lock and key controls for exterior doors, utility areas, elevator shafts and cars, fire escapes, and other potential targets should be stringent. Security and maintenance personnel should have a thorough understanding of the system and hardware used, and the level of security at each point. Doors not typically used for access should be inspected regularly.

Before the installation of locks of any kind, the doors should be inspected: their types and conditions may limit the locking options. For example, double doors and those with wooden frames may require double dead-bolt or long-throw locks. (BDC Editor's Note: Lock and key specifications are not detailed in this pamphlet. There are many methods and products available, and BDC participants should work with the appropriate professionals to determine the most feasible procedures and apparatus.)

Whenever conventional locks are used, all keys should be controlled. Provision should be made for the issuance of keys and their security when not in use. Various means can be used to prevent loss or theft. Biting numbers and similar data, for example, can be removed from the keys; this makes duplication more difficult. If feasible, the agency may prohibit removal of keys from the premises or attach them to heavy rings or chains that are not easily hidden or misplaced.

If the perceived threat so warrants, rolling metals doors ("riot doors") can be installed to some or all entrances. If these are electrically powered, the circuitry and apparatus will need to be secured.

Windows: There are several methods available to protect glass windows, often a target for bombers. They include: the installation of bars and grilles, the replacement of sills and ledges with angled surfaces, and the replacement of glass with polycarbonate or plate glass products. In extreme circumstances, existing window openings can be sealed or bricked over, although this can cause appearance and personnel problems. In some cases, it may be financially or practically infeasible to modify all windows. In these cases, windows may be selected on the basis of vulnerability for additional security measures.



Identification & Interior Movement Control

1. [Personnel Entry & Monitoring](#)
2. [Visitor Access](#)
3. [Vehicle Control](#)
4. [Material Control](#)

Personnel Entry & Monitoring

Consistent and exacting identification is the cornerstone of personnel control. The efficiency of the program will depend on the accuracy of identifications as well as the uniform application of procedures.

Personal Identification - While this is the best means of positive identification, it is only applicable when the number of authorized personnel is small and they enter the premises sporadically. Furthermore, the system depends heavily on reliable identifiers who are present every day. Even when it is used, personal identification should be augmented with another system, such as credential (badge, pass, etc.) verification.

Artificial Access Identification Systems - There are several types of pass systems which may be used. The actual credentials may incorporate identifying numbers, signatures, various encodements, and photographs. Some of the ways in which they may be used are discussed below.

Any credential system is only as secure as the items themselves, which are always subject to loss and theft, and often able to be altered or reproduced. The safeguarding policies and procedures of the manufacturer, where the security of the items begins, should be evaluated before a supplier is selected. Within the agency, one or more employees (as few as feasible) should be designated to audit the recording, dispersal, and collection of credentials as necessary. Compromised or otherwise unusable materials should be destroyed. A permanent record of all badges and their respective

dispositions should be kept. Periodic reviews of this record and the credential inventory may be instigated.

A single pass system permits access after the employee presents the appropriate credential in the prescribed manner. The system can be modified by the use of encodements on the badge or pass: a color or numbering system designating specific times or areas of access, for example. (BDC Editor's Note: Technology in this field is expanding rapidly, and the apparatus becoming more sophisticated as well as "user-friendly". Security personnel should keep this in mind when purchasing or leasing equipment.)

An exchange system involves the use of two items for each employee. One pass is tendered to a guard upon entry and its data compared to that on a pass retained at the access point. If the credentials correspond, the second one is given to the employee to wear on the premises. The procedure is reversed for leaving. This system, if it is consistently and rigidly maintained, can minimize the effect of lost credentials.

A multiple pass system may be used to augment whatever entry system is used. In this case, additional credentials are required for specific, sensitive parts of the structure or premises.

Combination locks, in which a sequence of numbers is entered by turning a dial or using a push-button panel, can also be used. Often their combinations can be changed by agency personnel. These electronic systems are available in many degrees of complexity; some incorporate failsafe mechanisms into their construction. For example, some push-button types will signal when a large number of incorrect sequences are attempted in a specified interval, minimizing the possibility of unauthorized entry through experimentation. A variant of this kind of lock requires the use of an encoded pass, placed in a receptacle to trigger the lock. Some systems will sound an alarm if an improper card is inserted.

Lock and key access, either traditional or electronic, is particularly useful for interior access denial. Keys or combinations are given only to those with a need to access a specific area. Alternatively, employees working in the sensitive area are provided with a keyed entry, while employees from other parts of the organization pass through a separate, guarded entrance.

[Contents](#)

Unmanned systems are susceptible to breaching by unauthorized individuals entering with employees. A physical barrier, such as a turnstile permitting single-file access, may be feasible. If not, employees should be cautioned not to let unauthorized people into the secured area: measures to forestall forcing entry by this means should be implemented.

Visitor Access

The scope and complexity of visitor control will be dictated to a great extent by the type of business conducted and the security levels necessary. In any case, security procedures for visitors should be unobtrusive and done in a pleasant manner. The reputation of the agency is never enhanced when visitors are made to feel defensive. There are several methods by which visitors can be discreetly screened.

When minimal security is needed, visitors can be admitted if their stated purposes are feasible, and the identifying guards have no reason to question their intent. Verification of the visit by contacting the employee to be seen provides additional security. In any case, items being carried by visitors should be examined at the time of entry.

Following entry, the visitor may be directed or escorted to the appropriate office. In the first case, the guard desk is notified when the visitor arrives; if notification does not occur within a specified interval, a search is begun. In the latter circumstance, the escort can be either a guard designated guide, or an employee of the destination office. The prevailing security level and the physical layout of the premises will dictate whether either of these means is feasible.

Security may be increased by requiring visitors to sign in and out, usually by entering specified data (name, affiliation, signature, etc.) in a control log. Temporary badges may be issued in concert with the log. This is particularly expedient if the visitor regularly frequents the premises for business purposes. The credential can be similar to the type used by employees, but encoded with more restriction. Infrequent visitors can also be issued a pass in conjunction with the log. These credentials should be differentiated by color or design from those of employees and quasi-official visitors: spaces to write in names, time, and other relevant data should be provided. Whatever procedures are used for visitors, they should be easily and expeditiously completed. Cumbersome practices will be "streamlined" by implementing personnel, with a consequent loss of consistency and security.

Vehicle Control

All vehicles, both employees' private cars and service vans, entering secured areas should be monitored and scrutinized. Before implementing these procedures, however, security planners should note any sensitive areas that are adjacent to public vehicle thoroughfares or parking spaces. For example, a booby-trapped car parked in a public loading zone can cause substantive damage, when it explodes, to the adjacent structure, even if a chain link fence and several armed guards separate them. The installation of structural barriers or movement of critical functions might be indicated.

With respect to on-site vehicles, security personnel should familiarize themselves with employee traffic patterns, and the usual hours and duration of commercial vehicle-related activities (deliveries, trash removal, etc.). For security purposes, a log of arrivals and departures can be implemented or vehicles may be inspected. The log can be used to determine what patterns of activity and to isolate deviations.

The same kinds of accessing techniques used for individuals can, with a few modifications, monitor and limit vehicle access.

Material Control

It is prudent to formulate an inspection policy for items coming into the agency. This includes mail, briefcases, parcels, etc. (BDC Editor's Note: The BDC has compiled a bulletin, General Information Bulletin 83-4, which discusses the recognition and handling of suspicious posted items. The bulletin, which includes a poster highlighting its main points, is available for training purposes from the BDC.)

Items being brought into the secured area can be manually inspected, although the method is time-consuming and may annoy visitors. Spot searches of this kind can be done, but this will reduce the effective security significantly. Inspections using a portable X-ray machine or scanner may be more viable. There are a variety of commercial items available. Radiographic inspections of everything that is brought in may be expensive, however, or may subject employees to levels of radiation that they find unacceptable.

One way to avoid a bottle-neck for examination of parcels in an access area is to detain those individuals with carried items until traffic is light, or route them through a different area.

Structural Enhancement of Security Measures

Only under ideal circumstances are security personnel privy to new construction plans. They are, however, often able to suggest retrofitting that will enhance the physical security of an existing structure. Many aspects of construction that affect security have been previously discussed; this section will address those which have not been covered.

Means of Access - Only essential entryways should be provided. Stairways provide myriad hiding places for bomb devices, and ground level entrances should be planned to avoid their use. Ramps can sometimes be substituted. (BDC Editor's Note: This will have the added advantage of streamlining access for handicapped persons.) If stairs must be used, there are functional, open types available which will minimize niches, corners, and other hiding places. They need not be unattractive.

As previously mentioned, windows on accessible floors may be eliminated to prevent items being thrown into the structure. Closing existing doors and windows is often unacceptable aesthetically or with respect to employee needs. A viable compromise can sometimes be reached. (It is essential that security needs be evaluated in conjunction with other priorities. A practice that is perceived to be undesirable will not be followed consistently or willingly.)

Interior Stairwells - There are several ways to monitor or limit access to stairwells, another excellent place of seclusion of hazardous items. Fire codes are of paramount importance, and must be followed to assure employee safety and satisfy legal requirements. On occasion, they can be used to enhance security. For example, the fire marshal or other regulating authority may specify that all stairwells end at the lobby level, proceeding up or down from there. This provides a single entry point from which all individuals in the system can be monitored. Provisions must be made in this instance to preclude access between the two stairwells without entering a lobby or other visible area.

Elevators - Many of the principles concerning stairways and wells also obtain for elevators. They can, for example, be programmed to run between a specific number of floors. Many skyscrapers utilize different cars and shafts to access specific portions of the structure. [See Figure 2.](#)

One security consideration within a multibusiness structure is the use of access stairs or elevators by a firm occupying more than one floor. Monitoring movement can become difficult in this circumstance. For example, it is possible for an individual to enter an agency from one elevator bank, and use an access stair to attain an adjacent floor serviced by a different bank. The fire regulations for installation and use of these stairs are often exacting and, can, under some circumstances, be used to implement security measures. It is necessary for building security personnel and the specific occupants of the space to work out a viable plan.

Security personnel should be aware of the many methods of monitoring elevator traffic. Installation of a master elevator car panel in the central guard station can facilitate this. This will permit security personnel to note discrepancies between stated destinations and actual floors entered (particularly germane in the case of a visitor.)

The interiors of elevator cars can be designed to provide adequate, nongarish lighting without having hiding places such as lamp recesses or removable grilles. Trap doors into maintenance areas and emergency telephone cabinets should be equipped with alarms indicating when they are opened. Elevator shafts and machinery rooms should be afforded the appropriate security.

The situation of a well-equipped, visible guard station in the main lobby area of the structure will permit security personnel to maintain knowledge and control of activities throughout the elevator and stair system. The aforementioned panel is useful, as is a means of locking doors in different parts of the structure when an unauthorized entry attempt is made. If this station is to be enclosed, security personnel should consider the use of polycarbonate or another, resistive, transparent paneling.

Rooftop Equipment - While many structures have mechanical

equipment rooms (MER) inside, machinery is sometimes also situated on the roof. See Figure 2. Transformers may also be placed atop the structure. Rooftop mechanical equipment can provide a means for access to the building: if the items are enclosed, entry to the rooms should be susceptible to monitoring against unauthorized entry. Roof guards can be utilized, but they should not be visible from the ground.

Since access to interior MER areas will be limited as a matter of routine, security is uncomplicated to arrange and can be stringent.

New Construction

If security personnel will be working in a new structure or one that has undergone extensive remodeling, it may be possible to incorporate features that will help implement security upon its completion. It is easier and less expensive, for example, to add sources of electrical power and supportive components for a computerized entry and exit system while a building is in the framework stage. Most modern steel frame structures permit great leeway in the placement of interior partitions and security planners may be able to specify the configurations of some lobby and hall areas.

There are some facets of basic construction that can help or hinder security efforts. Responsible personnel should be aware of them, even though they will probably not be able to effect changes in overall plans. For example, the optimum structure with respect to security is a rectangular, unattached box. This is also the easiest and most cost-effective for the builder. However, this type of structure does not provide for many windows, an unusual lobby atrium, or other amenities that are important to the occupants. The unarticulated exteriors of the Bauhaus style are not popular among many modern designers: the most current style includes facades with column, alcoves, etc. If a compromise between aesthetics and security cannot be reached, at least personnel should be aware of the existence of niches, corners, etc.

Reinforced concrete is an excellent building material that will provide protection against a bomb blast. It is, furthermore, consistent with the current style of molded, articulated facades.

[Contents](#)

A modern structure may be fabricated around a steel framework, over which sheathings of other materials are placed to form interior and, less frequently, exterior walls. Under these circumstances, a crawl space between framework and wall may exist. Access to this should be impossible, or, if necessary, susceptible to careful monitoring. (BDC Editor's Note: These spaces often concern fire regulating and control agencies. It may be feasible to work with them on security and safety plans.)

Security planners should be familiar enough with the structural features of their areas of responsibility that they can identify likely problem spaces.

Figure 2.

**Permission of the International Society of Fire Service
Instructors from High Rise FireFighting Seminar
Manual, Page 53.**

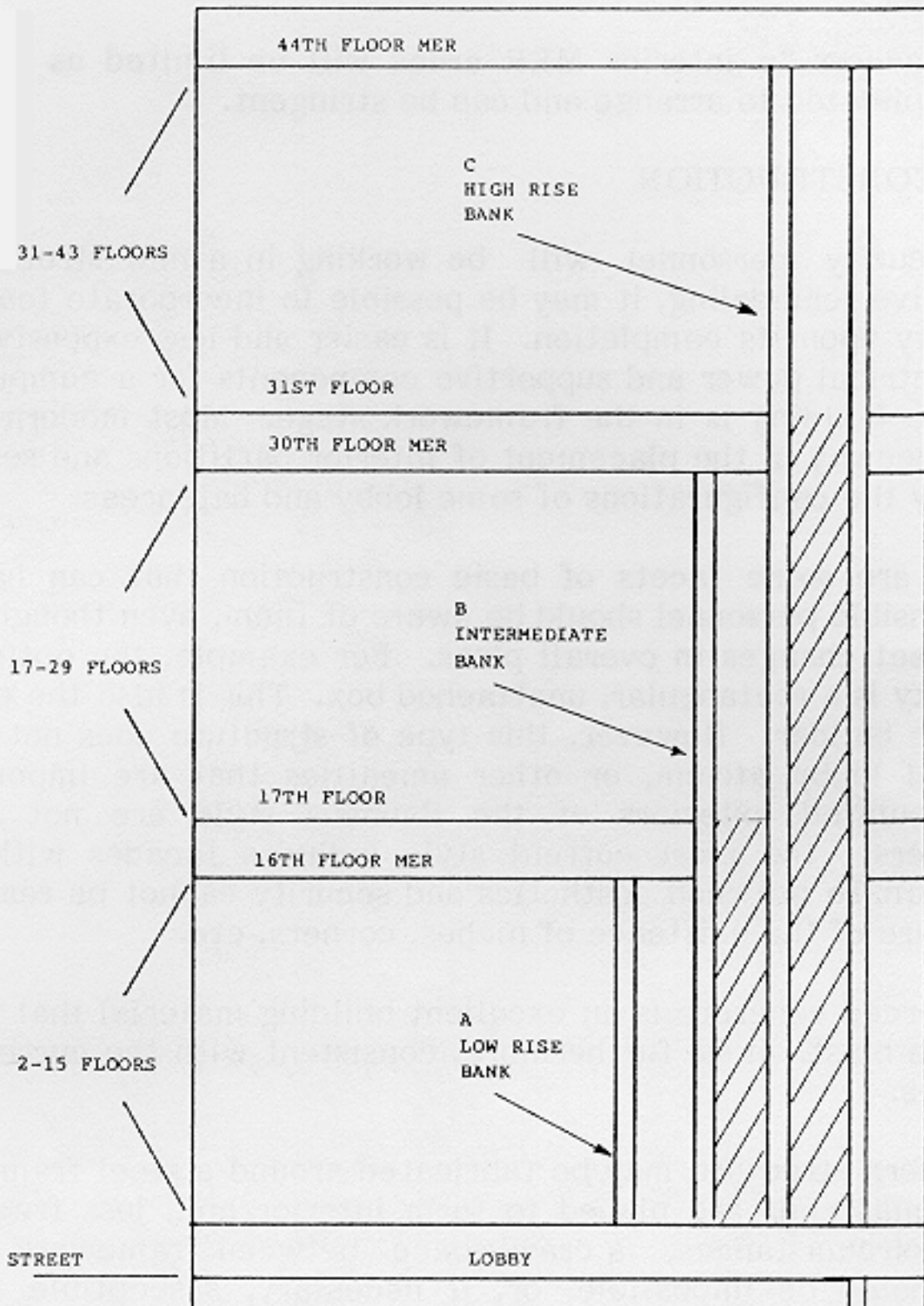


Figure 1

STREET

LOBBY

B-1

B-2

MER - MECHANICAL EQUIPMENT ROOM

HATCH = BLIND SHAFT

D
BASEMENT
BANK

Appendix: Security Plan for Preventing Bomb Attacks

A. Concept

1. In order to deny access to bombers and saboteurs, various security devices have been installed and measures implemented to protect the occupants and contents of the structures, and to ensure that vital operations will continue if an attack does occur.
2. Security plans will be revised when appropriate, and the specific measures in effect at a given time may vary according to the circumstances.
3. The cooperation of each employee in supporting this plan is essential, as some security measures will entail personal inconveniences and delays.

B. Scope

Describe exact physical premises and operations included in the plan.

C. Implementation

The plan will be implemented upon order of the (manager, chief, etc.) or a designated representative. Command and control during an incident will be vested with the (security officer, designated commander, etc.).

[Part 1: Critical Areas and Equipment; Special Security Provisions](#)

[Part 2: Procedures for Alert Condition 1](#)

[Part 3: Procedures for Alert Condition 2](#)

[Part 4: Procedures for Alert Condition 3](#)

[Contents](#)

Critical Areas (In Order of Importance)

Critical Areas	Location
Transformer	underground vault in building alcove, on the west.
Transformer Switch Gear	Room 100
Emergency Generator	Room 115
Emergency Operations Center (EOC)	Basement Room 3
Radio Equipment Room	Adjacent to EOC
Telephone Equipment Room	Adjacent to EOC

Special Security Provisions

1. Transformer Vault

A chain-link fence and gate, with appropriate lock, have been installed at the alcove entrance; the entrances to the vault have been secured; electronic intrusion detection devices have been installed; access is controlled by the EOC.

2. Stairwell cages

Cages, protected by electronic intrusion devices, have been installed in stairwells at ground level landings, which will prevent unauthorized basement entry, while providing stairwell access for those in the basement.

3. Closed Circuit Television

Closed circuit television systems, with moving image sensors, have been installed to monitor the elevator lobby at the entrance to the EOC.

4. Package Holding Areas

Blast-resistant package holding areas have been installed at ground level and

adjacent to a first floor entranceway.

5. Security Door

An additional door, which provides a means of emergency exit from the area, has been installed at one end of the hallway. It may be opened only by means of a panic bar on one side. It must not be blocked. (BDC Editor's Note: This is comparable to any emergency door, such as a fire exit to a stairwell. Such means of egress may be alarmed.)

6. Elevators

Lockout switches for the elevator cars and floors, and a car indicator panel, have been installed in the EOC. During security hours, elevator access to the basement is limited and monitored by the EOC.

7. Entrances and Fire Exits

All locks are in working order. Remote entrances have been alarmed.

8. Security Hours Entrance

Hours have been specified during which access to the building is limited to one entrance. (BDC Editor's Note: For large complexes, having several entrances and a multiplicity of personnel on different shifts, access at each entrance may be limited to different periods of time. Such a system is complicated and expensive, however, if mechanical accessing equipment, such as key cards, is used. The apparatus must be installed at every entrance.)

9. Wire

Standard concertina barbed wire has been prestocked for use as an emergency barrier, if needed.

10. Bomb Handling Equipment

The EOC is stocked with bomb blankets, X-ray machine, etc.). Type and number of items should be specified, as well as any procedures for obtaining them when needed.

11. EOC Guard

Provision has been made for a guard post in the lobby, outside the EOC. Telephone lines have been installed.

12. Employee Identification

All employees have been issued (photo badges, key cards, etc.). Specify procedure for use.

13. Security Lighting

Security lighting has been installed around the building to provide a uniform level of illumination.

14. Restrooms

Doors to restrooms in the basement are not identified as such and are accessible only by key.

15. Stairwell Doors

Stairwell doors have been provided with locking mechanisms consistent with local fire regulations.

Alert Condition 1

1. Instruct all employees to:

- a. Be alert for suspicious activity.
- b. Look for objects which are conspicuously out of place, or foreign to the area.
- c. Ensure that visitors do not leave packages or other objects in the building.
- d. Report and LEAVE UNTOUCHED any object foreign to the area.
- e. Report to EOC the arrival of outside maintenance or service personnel.
- f. Deny admittance of outside maintenance or service personnel to critical areas until identities have been verified, and the purpose of the visit authenticated.
- g. Observe and record the distinguishing characteristics of suspicious individuals and vehicles.
- h. Omit specific security plan details from their conversations.

2. Report unusual or suspicious incidents or individuals to the EOC.

3. Search Teams

Organize search teams for each shift.

4. Test

Require daily testing of all security devices (i.e., electronic intrusion detection devices); record results and keep in repair.

5. Exterior lighting

Lamps are to be replaced at 80% of the rated life. The lights, which are turned on during hours of darkness, should be kept clean and in good repair. Weekly inspections addressing the security of their controls should be

conducted.

6. Exterior Building Patrol

At least once an hour, on a random basis, inspect for evidence of tampering, verify security of critical areas, and be alert for suspicious or out of place items. REPORT SUCH ITEMS, DO NOT TOUCH THEM. Report burned out lights. Be alert for loiterers.

7. Interior Building Patrol

A continuous patrol of public areas should be maintained. Ensure that doors to closets, supply rooms, etc. are closed and locked. Check stairwell cage doors and locks for evidence of tampering; question suspicious persons. Ensure that fire exits are not obstructed.

8. Emergency Equipment

Periodically test, and verify the presence and serviceability of emergency communications equipment, electrical power sources, lighting, and fire equipment; i.e., extinguishers, standpipes, and first aid supplies.

9. Maintenance

Do not permit trash to accumulate in or around the building.

10. Badge Control and Access

Specify standard procedures, such as: during other than normal hours of operation, all individuals must sign in and out of the structure. In addition, employees must present identifying badges. Include a procedure for employees who have forgotten or lost their badges. Specify hours during which visitors will be admitted. Specify types of identification or verification used for admission of service and maintenance personnel; these individuals may be escorted, if the situation warrants.

11. Elevators

Lock all elevators off in the EOC thirty (30) minutes after the close of business. (BDC Editor's Note: If this is not feasible, lock only a portion of the cars, so that access is limited and controllable.) Turn elevators on forty-five (45) minutes before the structure opens for business. A telephone number



may be provided for individuals requiring the elevators at other times.

Alert Condition 2

In addition to the preventive measures prescribed for alert condition 1, the following procedures will be implemented by the proper authority.

1. During normal hours of operation, only two entrances will be kept open. Employees will be admitted upon presentation of their photo badges. Packages may be examined at the discretion of the guard on duty. Visitors will be screened or escorted to the appropriate part of the building.
2. Access to the EOC will be limited to those individuals named on a list. Official visitors and maintenance and service personnel must be escorted at all times while working in the EOC area.
3. Vehicle access to the structure will be limited by the erection of movable barricades. All vehicles seeking access will be screened prior to movement of the barricade.
4. The shipping and loading dock area will be guarded when the entrance is open.
5. Personnel access doors in elevator tops will be sealed.
6. Stairwell doors will be secured in accordance with fire regulations.
7. During other than normal business hours:
 - a. Guards (specify number) will be on duty at ground level.
 - b. Exterior patrols of the building will be conducted at least twice an hour, using different routes and a random schedule.
8. Guard personnel will be immediately available to the EOC to respond to reports of suspicious activity in or around the building.

Alert Condition 3

In addition to the measures prescribed for alert conditions 1 and 2, the following procedures will be implemented by the proper authority.

1. All individuals seeking entry to the building will be screened.
2. All packages which could conceal a bomb will be searched or checked in the holding areas at the ground and first level entrances.
3. The administrators of the services which occupy each floor are responsible for:
 - a. Implementing restroom and stairwell landing inspections (specify interval) for suspicious individuals or objects.
 - b. The monitoring of nonemployees in the area.
 - c. Denying unauthorized individuals access to office areas where they would be unobserved.
 - d. The prompt reporting of any suspicious activity or object to the EOC.